Defense Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2023 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Defense Cyber Security Market size is estimated at USD 22.95 billion in 2024, and is expected to reach USD 41.94 billion by 2029, growing at a CAGR of 12.82% during the forecast period (2024-2029).

Key Highlights
-Cyber threats are attempts made on the Internet to damage or disrupt Information Systems and steal critical information through various means, e.g., spyware and malware, as well as phishing. The landscape of defense networks in almost every country is changing due to the development of information technology and communication technologies. However, the threats are rapidly increasing as technology evolves. To safeguard data confidentiality, cybersecurity solutions provide defense organizations with the ability to monitor, detect, report, and deal with cyber threats.
-Over the last decade, a dynamic change has occurred within the defense industry. Reliable and enhanced cybersecurity solutions have been sought for the defense industry by increasing technological developments in information technology, improving existing weaponry with intelligence, surveillance, or a growing volume of classified data collected from different systems.
-Furthermore, cyber-attacks have become more frequent and sophisticated due to increased dependence on military organizations on the Internet. A significant focus is being put on adopting cybersecurity solutions within the defense sector to combat these vulnerabilities.
-Moreover, Past few years, the defense sector has undergone a wide range of changes. Reliable, more efficient cybersecurity solutions are needed for the defense sector due to increasing advances in information technology, the upgradation of old weapons with intelligence, surveillance, and an ever greater quantity of classified data collected from different systems.
-The growth of this market is expected to be hindered by factors such as a low priority for defense finance in some countries, coupled with the Return on Investment metrics, while factors such as the growing severity of cyber attacks against military or government organizations and an increasing commitment from governments to secure critical data.

-Amidst the rapidly shifting landscape in the wake of the COVID-19 pandemic, IT security teams in defense organizations are being faced with shoring up security in the face of increased attacks, on top of their regular responsibilities of managing risk and meeting compliance.

Defense Cyber Security Market Trends

Growing Severity of Cyber Attacks on Military/Government Organizations

- The number of attacks against governments, businesses, and individuals has increased by leaps and bounds. As attackers begin to realize the value in disrupting security systems that were once considered impenetrable, defense infrastructure is quickly becoming a target of choice among both individual and state-sponsored hackers.
- The growth of the market in this sector during the past decade has been driven by increased adoption of Machine-to-Machine Technologies within the aeronautics field, as well as a policy focus from governments aimed at increasing cybersecurity to counter cyber terrorism.
- Cyber attacks, which may have a devastating impact on the whole world, can be extremely vulnerable to navigation and guidance systems. Therefore, a robust safety infrastructure needs to be in place for computers and networks of all ground and air operations.
- As government and defense organizations expand operations to include the use of technologies such as the Internet of Things, mobile, and cloud, they inherently extend their cyber exposure. Data stratification in cyberspace extends throughout government and defense organizations, and regardless of the level of traditional security precautions, the cyber risk persists anywhere data exists. This creates a need to protect and manage private and sensitive information.
- In addition, to ensure the protection of important data, countries such as India are also stepping up their investment in cyber security systems.

North America is Expected to Exhibit a Significant Growth

- The United States, a major advanced economy, heavily relies on the Internet and has become particularly susceptible to cyber-attacks. At the same time, as well as being equipped with state-of-the-art technology and a sizeable military budget, this country has considerable defense capabilities. The United States continues to be at risk from malicious cyber attacks by its domestic or foreign enemies. The country has developed a strong cyber capability for its defense industry in response to these increasing threats.
- A significant market share of the defense cyber security market is projected to be held by Canada. The main drivers of demand in the country have been increased spending on cyber security, government initiatives for securing a computerized framework, and an emphasis on strengthening cybersecurity approaches.
- Furthermore, development in the business sector is being driven by building up cybersecurity units and installing powerful cyber defense systems in government organisations, military forces and security services.
- Also, Canada is home to major technological giants, which have been investing heavily in its cybersecurity R&D (Research and Development) initiatives to keep up with the heterogeneous nature of the cyber threats. The rising number of connected devices and rapid digitization in Canada is expected to drive the defense cybersecurity market in the country in the forecast period.

Defense Cyber Security Industry Overview

The defense cyber security market is highly competitive. Some major players in this industry are Northrop Grumman Corporation, Raytheon Technologies Corporation, Thales S.A., Boeing Company, IBM Corporation, and Cisco Systems Inc., among others. The defense cyber security market is a highly regulated industry that depends on government regulations and initiatives for any change in its dynamics.

In July 2023, Raytheon Company announced a new mentorship agreement with Node.Digital. It is a company specializing in digital transformation, intelligent automation, and artificial intelligence/machine learning services under the Department of Homeland Security's Mentor-Protege Program, where Raytheon will work with Node.Digital on capturing new business, positioning them to bid as a prime and mitigating program risk. Raytheon will support them in enhancing their capability to participate in advanced programs with complex cybersecurity engineering requirements and Node. Digital will receive guidance on business development strategy, engineering, and strategic planning processes.

In April 2023, SAIC was selected for a USD 889 million contract by the (FEDSIM) in support of (DCSA) in order to develop and implement One IT. IT modernization to DCSA's systems will be carried out by one IT. SAIC (Science Applications International Corporation) is to provide DCSA with support as a prime contractor for One IT to simplify and standardize its information technology environment with a view to ensuring that it is cloud-ready. SAIC's work will include planning and systems architecture development; digital; network, database, and storage engineering; service desk support; cybersecurity and IT application development and sustainment.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Defense Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2023 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature